IN THE CLAIMS

Please amend the claims as follows:

Claim 1 (Currently Amended): A transmitter device which transmits first data to a receiver device by driving a recording medium that stores the first data and second data that describes a limitation on the usage of the first data, the transmitter device comprising:

storage means for storing ~~an encrypted~~ a check value ~~of~~ calculated on the basis of the second data;

communication means which, in the authenticating of the receiver device, transmits the second data to the receiver device while receiving ~~an encrypted~~ a check value calculated on the basis of the second data from the receiver device; and

determination means which, in the authenticating of the receiver device, determines whether the ~~encrypted~~ check value of the second data received by the communication means matches the ~~encrypted~~ check value of the second data stored in the storage means to detect whether the second data is tampered with or not.

Claim 2 (Currently Amended): A transmitter device according of Claim 1, wherein the storage means inhibits the writing or reading of the ~~encrypted~~ check value of the second data in a process other than the authentication process.

Claim 3 (Original): A transmitter device according to Claim 1, wherein the storage means has a tamper resistance.

Claim 4 (Currently Amended): A transmitting method of a transmitter device which transmits first data to a receiver device by driving a recording medium that stores the first

data and second data that describes a limitation on the usage of the first data, the transmitting method comprising:

the step of storing ~~an encrypted~~ a check value calculated on the basis of the second data;

in ~~the~~ an authenticating step of the receiver device, the step of communication for transmitting the second data to the receiver device and for receiving ~~an encrypted~~ a check value calculated on the basis of the second data from the receiver device; and

in the authenticating of the receiver device, the step of determining whether the ~~encrypted~~ check value of the second data received in the communication step matches the ~~encrypted~~ check value of the second data stored in the storing step to detect whether the second data has been tapered with or not.

Claim 5 (Currently Amended): A program storage medium for storing a transmission process program for transmitting first data to a receiver device by driving a recording medium that stores the first data and second data that describes a limitation on the usage of the first data, the program executed by a transmitter device and comprising:

the step of storing ~~an encrypted~~ a check value calculated on the basis of the second data;

in ~~the~~ an authenticating step of the receiver device, the step of communication for transmitting the second data to the receiver device and for receiving ~~an encrypted~~ a check value calculated on the basis of the second data from the receiver device; and

in the authenticating of the receiver device, the step of determining whether the ~~encrypted~~ check value of the second data received in the communication step matches the ~~encrypted~~ check value of the second data stored in the storing step to detect whether the second data has been tapered with or not.

Claim 6 (Currently Amended): A receiver device for receiving first data from a transmitter device, the receiver device comprising:

communication means which, in the authenticating of the transmitter device, receives, from the transmitter device, second data that describes a limitation on the usage of the first data while transmitting ~~an encrypted~~ check value calculated on the basis of the second data to the transmitter device; and

encrypted value generator means for generating the ~~encrypted~~ check value of the second data based on the second data received by the communication means, in the authenticating of the transmitter device, said check value for detecting whether the second data has been tapered with or not.

Claim 7 (Currently Amended): A receiver device according to Claim 6, further comprising random number generator means for generating a random number having a predetermined bit number, wherein the communication means transmits, to the transmitter device, the ~~encrypted~~ check value of the second data together with the random number generated by the random number generator means.

Claim 8 (Currently Amended): A receiver device according to Claim 6, further comprising usage limiting data generator means which generates, subsequent to the reception of the first data, third data which describes a limitation on the usage of the first data, based on the second data received by the communication means,

wherein the encrypted value generator means generates ~~an encrypted~~ a check value generated on the basis of the third data generated by the usage limiting data generator means, and

the communication means transmits, to the transmitter device, the ~~encrypted~~ check value of the second data together with the ~~encrypted~~ check value of the third data.

Claim 9 (Currently Amended): A receiving method of a receiver device for receiving first data from a transmitter device, comprising:

in the authenticating of the transmitter device, the step of communication for receiving, from the transmitter device, second data that describes a limitation on the usage of the first data and for transmitting ~~an encrypted~~ a check value calculated on the basis of the second data to the transmitter device; and

in the authenticating of the transmitter device, the step of generating ~~an encrypted~~ a check value of the second data based on the second data received in the communication step, said check value for detecting whether said second value has been tampered with or not.

Claim 10 (Currently Amended): A program storage medium for storing a reception process program for receiving first data from a transmitter device, the program executed by a receiver device and comprising:

in the authenticating of the transmitter device, the step of communication for receiving, from the transmitter device, second data that describes a limitation on the usage of the first data and for transmitting ~~an encrypted~~ a check value calculated on the basis of the second data to the transmitter device; and

in the authenticating of the transmitter device, the step of generating ~~an encrypted~~ a check value of the second data based on the second data received in the communication step, said check value for detecting whether said second value has been tampered with or not.

Claim 11 (Original): A communication system comprising a transmitter device which transmits first data by driving a recording medium that stores the first data and second data that describes a limitation on the usage of the first data, and a receiver device for receiving the first data;

the transmitter device comprising:

storage means for storing ~~an encrypted~~ a check value ~~of~~ calculated on the basis of the second data;

first communication means which, in the authenticating of the receiver device, transmits the second data to the receiver device while receiving ~~an encrypted~~ a check value calculated on the basis of the second data from the receiver device; and

determination means which, in the authenticating of the receiver device, determines whether the ~~encrypted~~ check value of the second data received by the communication means matches the ~~encrypted~~ check value of the second data stored in the storage means; and

the receiver device comprising:

second communication means which, in the authenticating of the transmitter device, receives, from the transmitter device, second data that describes a limitation on the usage of the first data while transmitting ~~an encrypted~~ the check value calculated on the basis of the second data to the transmitter device; and

encrypted value generator means for generating the ~~encrypted~~ check value of the second data based on the second data received by the communication means, in the authenticating of the transmitter device, said check value for detecting whether the second data has been tapered with or not.

Claim 12 (New): A transmitter device for transmitting a content to a receiver device comprising:

a memory configured to store a hash value of a content management data in relation to said content;

communicating means for transmitting said content management data of said content and receiving a hash value calculated at said receiver device on the basis of said content management data from said receiver device;

comparing means for comparing said check value in said storage and said check value transmitted from said receiver device; and

determining means for determining whether said content management data is tempered or not, on a basis of a result provided by the comparing means.

Claim 13 (New): The transmitter device according to claim 12, wherein said content management data is changed when said content is used and the status of said content is changed.

Claim 14 (New): The transmitter device according to claim 12, wherein said management data is changed when said content is used and the status of said content is changed.

Claim 15 (New): The transmitter device according to claim 12, wherein said content management data is in accordance with at least one of a reproduction of said content, a copying of said content, and a movement of said content.

Claim 16 (New): The transmitter device according to claim 15, wherein said content management data is at least one of a number of said reproduction of said content and a number of the copying of said content.

Claim 17 (New): The transmitter according to claim 12, further comprising:

controlling means for controlling said communicating means to transmit said content to said receiver device when said determining means determines that said content management data has not been tampered with.

Claim 18 (New): A computer implemented program that when executed by a processor implements steps comprising:

storing a check value of a content management data in relation to said content;

transmitting said content management data of said content and receiving a check value calculated at a receiver on the basis of said content management data from said receiver;

comparing said check value stored in said storing step with said check value transmitted from said receiver; and

determining whether said content management data has been tampered with or not, on a basis of a result by the comparing step.

Claim 19 (New): The program of claim 18, wherein said content management data indicates an authorized usage of said content data.

Claim 20 (New): The program according to 18, wherein said content management data is changed when said content is used and a status of said content is changed.

Claim 21 (New): The program of claim 18, wherein said content management data is in accordance with at least one of a reproduction of said content, a copying of said content, and a movement of said content.

Claim 22 (New): The program according to claim 21, wherein said content management data is at least one of a number of said reproductions of said content and a number of copies of the content.

Claim 23 (New): The program according to claim 18, further comprising:

controlling a transmitter that transmits said content management data in said transmitting step so as to transmit said content to said receiver when in said determining step it is determined that said content management data has not been tampered with.

Claim 24 (New): A method for transmitting a content to a receiver device comprising:

storing a check value of a content management data in relation to said content;

transmitting said content management data of said content and receiving a check value calculated at a receiver on the basis of said content management data from said receiver;

comparing said check value stored in said storing step and said check value transmitted from said receiver; and

determining whether said content management data has been tampered with or not, on a basis of a result by the comparing step.

Claim 25 (New): A program storage medium for storing a transmission process program for transmitting a content to a receiver device, said program storage medium including instructions that when executed by a transmitter device implement steps comprising:

storing a check value of a content management data in relation to said content;

transmitting said content management data of said content and receiving a check value calculated at a receiver on the basis of said content management data from said receiver;

comparing said check value stored in said storing step and said check value transmitted from said receiver; and

determining whether said content management data is tampered with or not, on a basis of a result of the comparing step.